CERT-MU Security Alert

CERT-MU

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: 13 July, 2016

Severity Rating: High

Description:

Multiple vulnerabilities have been identified in Microsoft products and they can be exploited by attackers to cause execution of arbitrary code, gain knowledge of sensitive information, take full control of the affected systems and bypass security restrictions. The vulnerabilities reported are as follows:

Vulnerability	Description	Affected Software	Workarounds
Multiple Vulnerabilities in Microsoft Internet Explorer **CVE Info:** CVE-2016-3204 CVE-2016-3240 CVE-2016-3241 CVE-2016-3242 CVE-2016-3243 CVE-2016-3245 CVE-2016-3248 CVE-2016-3259 CVE-2016-3260 CVE-2016-3261 CVE-2016-3264 CVE-2016-3273 CVE-2016-3274 CVE-2016-3276 CVE-2016-3277	Multiple vulnerabilities have been identified in Internet Explorer and could be exploited to cause execution of arbitrary code. These vulnerabilities can allow attackers to view specially crafted webpage using Internet Explorer. Successful exploitation of the vulnerabilities could allow gaining the same user rights as the current user.	Internet Explorer 9 Internet Explorer 10 Internet Explorer 11	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-084
Multiple Vulnerabilities in Microsoft Edge	Multiple vulnerabilities have been identified in Microsoft Edge and could allow remote	Microsoft Edge	Users are advised to apply updates. More

CVE Info: CVE-2016-3244 CVE-2016-3246 CVE-2016-3248 CVE-2016-3259 CVE-2016-3260 CVE-2016-3264 CVE-2016-3265 CVE-2016-3269 CVE-2016-3271 CVE-2016-3273 CVE-2016-3274 CVE-2016-3276 CVE-2016-3277	attackers to cause code execution if a user views a specially crafted webpage using Microsoft Edge. Successful exploitation of the vulnerabilities could gain the same user rights as the current user.		information about the updates is available in: https://technet.microsoft.com/library/security/MS16-085
Vulnerability in JScript and VBScript scripting engines in Microsoft Windows **CVE Info:** CVE-2016-3204	A vulnerability has been reported in JScript and VBScript scripting engines in Microsoft Windows. The vulnerability could allow remote code execution if a user visits a specially crafted website. Successful exploitation of the vulnerability could allow attackers to gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	Windows Vista Windows Server 2008	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-086
Multiple Vulnerabilities Windows Print Spooler Components **CVE Info:** CVE-2016-3238	Multiple Vulnerabilities have been identified in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker is able to execute a man-in-the-middle (MiTM) attack on a workstation or print server, or set up a rogue print server on a target network.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8.1 Windows Server 2012	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-087

		Windows Server 2012 R2 Windows RT Windows 10	
Multiple Vulnerabilities in Microsoft Office **CVE Info:** CVE-2016-3279 CVE-2016-3278 CVE-2016-3280 CVE-2016-3281 CVE-2016-3282 CVE-2016-3283 CVE-2016-3284	Multiple Vulnerabilities have been identified in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. Successful exploitation of the vulnerabilities could allow remote attackers to run arbitrary code in context of the current user.	Microsoft Office 2007 Microsoft Office 2010 Microsoft Office 2013 Microsoft Office 2013 RT Microsoft Office 2016 Microsoft Office for Mac 2011 Microsoft Office 2016 for Mac	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-088
Vulnerability in Windows Secure Kernel Mode **CVE Info:** CVE-2016-3256	A vulnerability has been identified in Microsoft Windows. The vulnerability could allow information disclosure when Windows Secure Kernel Mode improperly handles objects in memory.	Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-089
Vulnerability in Windows Kernel Mode Drivers **CVE Info:** CVE-2016-3249 CVE-2016-3250 CVE-2016-3251 CVE-2016-3252 CVE-2016-3254 CVE-2016-3286	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.	Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 Windows Server 2012 and Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-090
Vulnerability in .NET Framework **CVE Info:**	A vulnerability has been identified in Microsoft .NET Framework. The vulnerability could cause information	Windows Vista Windows Server 2008 Windows 7	Users are advised to apply updates. More information about the

CVE-2016-3255	disclosure if an attacker uploads a specially crafted XML file to a web-based application.	Windows Server 2008 R2 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10	updates is available in: https://technet.microsoft.com/library/security/MS16-091
Vulnerability in Windows Kernel **CVE Info:** CVE-2016-3258 CVE-2016-3272	A vulnerability has been identified in Microsoft Windows. The vulnerabilities could allow security feature bypass if the Windows kernel fails to determine how a low integrity application can use certain object manager features.	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-092
Vulnerabilities in Adobe Flash Player **CVE Info:** https://helpx.adobe.com/security/products/flash-player/apsb16-25.html	Vulnerabilities in Adobe Flash Player when installed on all supported editions of Windows 8.1, Windows Server 2012, Windows Server 2012 R2, Windows RT 8.1, and Windows 10.	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-093
Vulnerability in Secure Boot **CVE Info:** CVE-2016-3287	A vulnerability has been reported in Secure Boot. The vulnerability could allow Secure Boot security features to be bypassed if an attacker installs an affected policy on a target device. An attacker must have either administrative privileges or physical access to install a policy and bypass Secure Boot.	Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1 Windows 10	Users are advised to apply updates. More information about the updates is available in: https://technet.microsoft.com/library/security/MS16-094

Source:

Microsoft Security Bulletin

https://technet.microsoft.com/en-us/library/security/ms16-jul.aspx

Security Tracker

http://securitytracker.com/id/1036274

http://securitytracker.com/id/1036275

http://securitytracker.com/id/1036277

http://securitytracker.com/id/1036280

http://securitytracker.com/id/1036281

http://securitytracker.com/id/1036282

http://securitytracker.com/id/1036283

http://securitytracker.com/id/1036286

http://securitytracker.com/id/1036287

http://securitytracker.com/id/1036288

http://securitytracker.com/id/1036289

http://securitytracker.com/id/1036290

http://securitytracker.com/id/1036291

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu